FORME TRACE ET RAMIFICATION SAUVAGE

CHRISTINE BACHOC *et* BOAS EREZ

[Received 8 February 1989]

ABSTRACT

Let $A(K/\mathbb{Q})$ denote the fractional ideal of a cyclic p-extension $K/\mathbb{Q}$ whose square is the inverse different of the extension. Equipped with the trace form, $A(K/\mathbb{Q})$ becomes a $\mathbb{Z}\,\mathrm{Gal}\,(K/\mathbb{Q})$-hermitian module $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ with discriminant 1. By using results on the Galois module structure of $A(K/\mathbb{Q})$ and a classification of forms in cyclotomic fields, we show that if p is totally—and hence wildly—ramified in $K/\mathbb{Q}$, then the equivariant isometry class of $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ depends only on the degree of the extension.

0. *Introduction*

Soit $K/\mathbb{Q}$ une extension galoisienne de groupe de Galois G et de degré fini impair. Dans cet article nous poursuivons l'étude du $\mathbb{Z}G$-réseau $(A_K, \mathrm{Tr}_{K/\mathbb{Q}})$ obtenu en restreignant la forme trace

$$\mathrm{Tr}_{K/\mathbb{Q}}\colon K \times K \to \mathbb{Q}, \quad \mathrm{Tr}_{K/\mathbb{Q}}(x, y) = \mathrm{trace}_{K/\mathbb{Q}}(xy),$$

de l'extension $K/\mathbb{Q}$ à l'unique idéal A_K de K dont le carré est la codifférente $D(K/\mathbb{Q})^{-1}$. Rappelons que d'une part l'idéal A_K est le seul idéal rendant la forme trace unimodulaire (voir § 1.4), et que d'autre part la codifférente étant stable par l'action de G, A_K est un $\mathbb{Z}G$-module.

Soit $(\mathbb{Z}G, T_1)$ le $\mathbb{Z}G$-réseau où T_1 est la forme sur l'algèbre de groupe $\mathbb{Q}G$ pour laquelle les éléments de G forment une base orthonormale. Dans **[6–8]** on compare $(A_K, \mathrm{Tr}_{K/\mathbb{Q}})$ et $(\mathbb{Z}G, T_1)$, et en particulier on se demande quand ils sont isométriques.

Par définition une condition nécessaire pour l'existence d'une isométrie équivariante $(A_K, \mathrm{Tr}_{K/\mathbb{Q}}) \sim (\mathbb{Z}G, T_1)$ est que le module galoisien A_K soit isomorphe à $\mathbb{Z}G$. Il est montré dans **[6–8]** que si G est abélien, alors A_K est $\mathbb{Z}G$-libre si et seulement si l'extension $K/\mathbb{Q}$ est peu ramifiée: une extension abelienne $K/\mathbb{Q}$ est dite *peu ramifiée* si les premiers p de $\mathbb{Q}$ qui se ramifient sauvagement dans $K/\mathbb{Q}$ ont un indice de ramification égal à p: $e(p) = p$. Il s'avère que dans le cas abélien l'isomorphisme de $\mathbb{Z}G$-modules entre A_K et $\mathbb{Z}G$ (sans formes) entraîne l'existence d'une isométrie équivariante. En résumé on a donc le

THÉORÈME 0.1 **[6–8]**. *Soit $K/\mathbb{Q}$ une extension abélienne. Il existe une isométrie équivariante entre $(A_K, \mathrm{Tr}_{K/\mathbb{Q}})$ et $(\mathbb{Z}G, T_1)$ si et seulement si $K/\mathbb{Q}$ est peu ramifiée.*

Notre but est de montrer un analogue du Théorème 0.1 dans une situation où $K/\mathbb{Q}$ est très sauvagement ramifiée. Plus précisément on va considérer des extensions galoisiennes $K/\mathbb{Q}$ telles que:

(0.2) *le groupe de Galois $G = \mathrm{Gal}\,(K/\mathbb{Q})$ est un groupe cyclique d'ordre p^n, où $p \neq 2$ est un nombre premier, et n est un entier naturel, et de plus p se ramifie totalement dans $K/\mathbb{Q}$.*

Ce travail a été effectué lorsque le deuxième auteur bénéficiait d'une bourse du F.N.R.S. Suisse et de l'hospitalité de l'U.E.R. de Mathématiques de l'Université de Bordeaux 1.

A.M.S. (1980) subject classification: 12A57, 10C02.

Remarquons qu'aucune hypothèse n'est faite sur la ramification des nombres premiers autres que p.

Nous allons montrer le

THÉORÈME 0.3. *Soient $K/\mathbb{Q}$ et $K'/\mathbb{Q}$ deux extensions galoisiennes vérifiant* (0.2). *Alors pour toute identification des groupes de Galois* $\mathrm{Gal}(K/\mathbb{Q})$ *et* $\mathrm{Gal}(K'/\mathbb{Q})$ *on a une isométrie équivariante entre* $(A_K, \mathrm{Tr}_{K/\mathbb{Q}})$ *et* $(A_{K'}, \mathrm{Tr}_{K'/\mathbb{Q}})$.

La démonstration de ce théorème va suivre d'une description explicite d'un représentant 'abstrait' de la classe d'isométrie équivariante de $(A_K, \mathrm{Tr}_{K/\mathbb{Q}})$. Ainsi par exemple si l'ordre de G est p, l'extension est peu ramifiée et nous allons retrouver le fait que A_K possède une base orthonormale, i.e., A_K est isométrique à la forme standard $\langle 1, \ldots, 1\rangle$. Plus généralement si n est pair (respectivement impair) alors $A_K \sim \langle 1\rangle \oplus \mathcal{B}_n$ (respectivement $A_K \sim \langle 1, \ldots, 1\rangle \oplus \mathcal{B}_n$) où $\mathcal{B}_n$ est une forme unimodulaire, définie positive, paire, de rang $p^n - 1$ (respectivement $p^n - p$). Les vecteurs de longueur 2 dans $\mathcal{B}_n$ engendrent un système de racines $\mathrm{Rac}(\mathcal{B}_n)$ qui est de rang maximal; nous décrivons $\mathcal{B}_n$ dans la Proposition 6.6 et nous calculons $\mathrm{Rac}(\mathcal{B}_n)$ dans la Proposition 6.9.

Esquissons la preuve du Théorème 0.3. Soit $\mathcal{M}$ l'ordre maximal de $\mathbb{Q}G$. On commence par remarquer que les hypothèses (0.2) permettent de se ramener au calcul de la classe d'isométrie équivariante du plus petit sous-module de K contenant A_K qui soit stable par $\mathcal{M}$ (voir § 3). Ce module sera noté $\mathcal{M}A_K$. Il est essentiel pour cette étape de réduction que l'extension soit très sauvagement ramifiée et qu'un seul premier divise l'indice $[\mathcal{M}A_K : A_K]$. Il s'agit ensuite de montrer que la classe d'isométrie équivariante de $(\mathcal{M}A_K, \mathrm{Tr}_{K/\mathbb{Q}})$ ne dépend que des conditions (0.2). Nous utilisons le fait que $\mathcal{M}A_K$ est libre sur $\mathcal{M}$ (voir [**8**]), et nous nous ramenons à l'étude des formes sur $\mathcal{M}$.

On sait, que pour G cyclique d'ordre p^n, $\mathcal{M} \cong \bigoplus_{i=0}^{n} \mathbb{Z}[p^i]$, où $\mathbb{Z}[p^i]$ est l'anneau des entiers du corps cyclotomique $\mathbb{Q}(p^i)$ des racines p^i-èmes de l'unité. Nous sommes donc amenés à étudier des formes équivariantes dans les corps cyclotomiques et au § 4 nous allons classer certaines formes $\mathbb{Z}[p^i]$-équivariantes sur un idéal de $\mathbb{Q}(p^i)$ par un groupe $\mathcal{E}$ (voir la Proposition 4.2 et le Corollaire 4.6). A ce stade nous aurons besoin de la description en termes de sommes de Gauss des résolvantes d'un générateur libre de $\mathcal{M}A_K$ sur $\mathcal{M}$. Cette description nous permettra de repérer la forme qui nous intéresse dans le groupe $\mathcal{E}$.

En résumé notre travail aura donc consisté—encore une fois—à déduire la structure quadratique d'une connaissance précise de la structure galoisienne. Nous disons à la Remarque 5.6 comment on retrouve de la même manière les résultats de Conner et Perlis sur l'anneau des entiers (voir [**4**, Chapter IV]). Remarquons aussi que les calculs du § 2 permettent de déterminer l'ordre associé à A_K.

Le paragraphe 1 contient les définitions et les notations nécessaires. Le dernier paragraphe contient des exemples.

Après la rédaction de cet article nous nous sommes rendus compte que beaucoup d'idées que nous utilisons sur le lien entre forme trace et résolvantes se trouvent déjà dans l'oeuvre de A. Fröhlich et sont à la base de la théorie de son 'Pfaffien'. Nous invitons le lecteur à considérer notre travail comme une introduction à [**11**] et nos résultats comme un type de conséquences qu'il serait souhaitable de pouvoir en tirer.

Remerciements. Les auteurs remercient Jacques Martinet et Jacques Queyrut pour de stimulants entretiens ainsi que Eva Bayer pour les conseils permettant d'étendre les résultats de [**13**] à la situation plus générale considérée au § 4.

1. *Définitions et notations*

1.1. *Réseaux*

Soit G un groupe fini, F un corps de nombres et $\mathbb{Z}_F$ l'anneau des entiers de F. On s'interesse aux couples (V, b) où V est un FG-module de dimension finie sur F muni d'une forme

$$b\colon V \times V \to F$$

bilinéaire, symétrique et G-équivariante. C'est-à-dire que pour tout x et y dans V et pour tout g dans G,

$$b(g(x), g(y)) = b(x, y).$$

Toutes les formes considérées dans la suite seront non-dégénérées, c'est-à-dire d'adjoint injectif.

Un $\mathbb{Z}_F G$-*réseau* (R, b) dans (V, b) est un $\mathbb{Z}_F G$-module R contenu dans V et tel que $FR = V$. Soit $R = (R, b)$ un $\mathbb{Z}_F G$-réseau dans (V, b):

—le réseau *dual* de R est le $\mathbb{Z}_F G$-réseau

$$R^* = \{x \in FR \mid b(x, R) \subseteq \mathbb{Z}_F\}.$$

On sait que $(R^*)^* = R$.

—R est dit *entier* si $R \subseteq R^*$, ou de façon équivalente, si pour tout x et y dans R, $b(x, y)$ appartient à $\mathbb{Z}_F$;

—si R est entier on définit le *discriminant* de R comme étant l'indice

$$\operatorname{disc}(R) := [R^* : R],$$

c'est un entier positif si $F = \mathbb{Q}$.

—R est *unimodulaire* si $R = R^*$.

Soit maintenant $F = \mathbb{Q}$:

—le réseau entier R est *pair* si pour tout x dans R l'entier $b(x, x)$ est pair;

—R est *indécomposable* s'il l'est en tant que $\mathbb{Z}G$-module.

La forme b est *définie positive* s'il existe une isométrie définie sur le corps des réels $\mathbb{R}$ entre b et la forme standard $\langle 1, \ldots, 1\rangle$.

Deux $\mathbb{Z}G$-réseaux R dans (V, b) et R' dans (V', b') sont $\mathbb{Z}G$-*isométriques* s'il existe un isomorphisme de $\mathbb{Z}G$-modules $\phi\colon R \to R'$ tel que $b(x, y) = b'(\phi(x), \phi(y))$. On notera $R \sim R'$ et on parlera aussi d' *isométrie équivariante.* Nous notons par $\oplus$ une somme orthogonale.

1.2. *Corps de nombres*

Soit K/F une extension de corps de nombres. Pour un idéal premier P de K on note $v_P(J)$ la valuation en P de l'idéal J. Aussi $D(K/F)$ est la *différente* de l'extension K/F, définie comme étant l'inverse de l'idéal dual de l'anneau des

entiers $\mathbb{Z}_K$ pour la *forme trace*

$$\mathrm{Tr}_{K/F}\colon\ K\times K\to F,\quad \mathrm{Tr}_{K/F}(x,y):=\mathrm{trace}_{K/F}(xy).$$

Dans le cas où K/F est une extension galoisienne de groupe de Galois G la forme trace est G-équivariante et tout idéal stable sous l'action de G est un $\mathbb{Z}_F G$-réseau.

1.3. *Rappels sur l'algèbre $\mathbb{Q}G$ pour G cyclique d'ordre p^n*

Dans toute la suite $p\neq 2$ est un nombre premier. Soit G un groupe cyclique d'ordre $|G|=p^n$. On filtre G par la famille de sous-groupes H_i où H_i est d'ordre p^{n-i}:

$$G=H_0\supseteq H_1\supseteq\ldots\supseteq H_n=\{1\}.$$

Considérons les deux familles d'idempotents $\varepsilon=\{\varepsilon_i\}$ et $e=\{e_i\}$ $(0\leqslant i\leqslant n)$ définies par

$$|H_i|\,\varepsilon_i=\sum_{H_i} g\quad (0\leqslant i\leqslant n),$$

$$e_0=\varepsilon_0,$$

$$e_i=\varepsilon_i-\varepsilon_{i-1}\quad (1\leqslant i\leqslant n).$$

On vérifie aisément les propriétés suivantes:

(a) $\varepsilon_i^2=\varepsilon_i$ et si $j<i$ alors $\varepsilon_j\varepsilon_i=\varepsilon_j$;

(b) e est l'unique famille d'indempotents (centraux) orthogonaux de l'algèbre $\mathbb{Q}G$, c'est-à-dire que pour tout i, $e_i^2=e_i$, que si $i\neq j$ alors $e_ie_j=0$ et que de plus on a une décomposition $1=e_0+\ldots+e_n$ à laquelle correspond la décomposition en algèbres simples de $\mathbb{Q}G$:

$$\mathbb{Q}G=\bigoplus_i \mathbb{Q}Ge_i. \tag{1.1}$$

Notons par $\mathbb{Q}(p^i)$ le corps cyclotomique des racines p^i-èmes de l'unité et par $\mathbb{Z}[p^i]$ son anneau d'entiers. G agit sur $\mathbb{Q}(p^i)$ via multiplication par une racine de l'unité d'ordre p^i. Ceci donne des isomorphismes de G-modules

$$\chi_i\colon\ \mathbb{Q}Ge_i\cong\mathbb{Q}(p^i)\quad\text{et}\quad \mathbb{Z}Ge_i\cong\mathbb{Z}[p^i] \tag{1.2}$$

induits par l'évaluation d'un caractère irréductible χ_i de $\mathbb{Q}G$.

L'ordre maximal de $\mathbb{Q}G$ est

$$\mathcal{M}=\bigoplus_i \mathbb{Z}Ge_i. \tag{1.3}$$

A la décomposition (1.3) correspond la décomposition suivante du groupe des classes localement libres de $\mathcal{M}$ en termes des groupes de classes d'idéaux des corps $\mathbb{Q}(p^i)$:

$$\mathrm{Cl}(\mathcal{M})\cong\bigoplus_i \mathrm{Cl}(\mathbb{Z}[p^i]). \tag{1.4}$$

EXEMPLE 1.5. Considérons les formes suivantes.

(a) $V=\mathbb{Q}G$ muni de la forme $b=T_s$ définie comme suit: pour $z=\sum_G z(g)g$ dans $\mathbb{Q}G$, soit

$$\bar{z}:=\sum_G z(g)g^{-1}\quad\text{et}\quad \mathrm{pr}_1(z):=z(1),$$

alors pour $s=\bar{s}$ on définit T_s par $T_s(x,y):=\mathrm{pr}_1(sx\bar{y})$.

Remarquons que

$$|G|\,\mathrm{pr}_1(z) = \mathrm{trace}_{\mathbb{Q}G/\mathbb{Q}}(z). \tag{1.6}$$

(b) $V = \mathbb{Q}(p^i)$ muni de la forme

$$b(x, y) = \mathrm{tr}_{i,0}(\sigma x, y) := \mathrm{trace}_{\mathbb{Q}(p^i)/\mathbb{Q}}(\sigma x \bar{y}),$$

où $^-$ dénote la conjugaison complexe et σ dans $\mathbb{Q}(p^i)$ est tel que $\sigma = \bar{\sigma}$.

Avec ces notations on voit que la décomposition (1.1) est orthogonale pour T_s et que—grâce à (1.6)—les isomorphismes (1.2) sont des isométries:

$$|G|\,T_s(x, y) = \sum \mathrm{tr}_{i,0}(\chi_i(s)\chi_i(x), \chi_i(y)).$$

1.4. *Les réseaux $A_K^{\mathcal{M}}$, A_K et $\mathcal{M}A_K$*

Soit $K/\mathbb{Q}$ une extension galoisienne de groupe G. Pour la forme trace $\mathrm{Tr}_{K/\mathbb{Q}}$ le dual d'un idéal J de K est l'idéal

$$J^* = J^{-1}D(K/\mathbb{Q})^{-1}. \tag{1.7}$$

On voit que, si le degré de l'extension $K/\mathbb{Q}$ est impair, alors il existe un unique idéal $A_K = A(K/\mathbb{Q})$ dans K avec $A_K^2 = D(K/\mathbb{Q})^{-1}$: utiliser par exemple la formule donnant la valuation de la différente $D(K/\mathbb{Q})$ en termes des groupes de ramification

$$v_P(D(K/\mathbb{Q})) = \sum_{-1<j} (|G(j, P)| - 1) \tag{1.8}$$

(voir [**14**, IV.1, Proposition 4]). Il est clair par (1.7) que A_K est un $\mathbb{Z}G$-réseau unimodulaire.

Comme annoncé, le but de cet article est de décrire la classe de $\mathbb{Z}G$-isométrie du $\mathbb{Z}G$-réseau $(A_K, \mathrm{Tr}_{K/\mathbb{Q}})$ dans le cas où l'extension satisfait aux conditions (0.2) de l'introduction. On suppose désormais que $K/\mathbb{Q}$ est une telle extension. D'après [**6–8**], dans cette situation A_K n'est même pas $\mathbb{Z}G$-projectif (sauf si $n = 1$), c'est pourquoi on essaye d'abord de décrire la structure de A_K sur l'ordre maximal $\mathcal{M}$.

DEFINITION 1.6. On note $\mathcal{M}A_K$ le plus petit $\mathcal{M}$-module contenant A_K qui soit contenu dans K et on note $A_K^{\mathcal{M}}$ le plus grand $\mathcal{M}$-module contenu dans A_K:

$$A_K^{\mathcal{M}} \subseteq A_K \subseteq \mathcal{M}A_K.$$

Les $\mathcal{M}$-modules $\mathcal{M}A_K$ et $A_K^{\mathcal{M}}$ sont des $\mathbb{Z}G$-réseaux pour la forme trace; nous allons voir au § 3 qu'ils sont une bonne approximation de $(A_K, \mathrm{Tr}_{K/\mathbb{Q}})$. En effet de manière générale on peut montrer que $[A_K : A_K^{\mathcal{M}}]$ et $[\mathcal{M}A_K : A_K]$ sont des puissances de p qui diminuent quand l'indice de ramification de p dans K augmente.

2. *Propriétés des $\mathbb{Z}G$-réseaux $\mathcal{M}A_K$ et $A_K^{\mathcal{M}}$*

Ce paragraphe décrit les réseaux $\mathcal{M}A_K$ et $A_K^{\mathcal{M}}$ définis plus haut. En particulier nous donnons ici leur décomposition en somme de $\mathbb{Z}G$-réseaux indécomposables et nous faisons le calcul de leur discriminant.

PROPOSITION 2.1. (1) *Comme A_K est unimodulaire on a*

$$(A_K^{\mathcal{M}})^* = \mathcal{M}A_K.$$

(2) *A la décomposition* (1.3) *de l'ordre maximal correspond la décomposition*

$$A_K^{\mathcal{M}} = R_0 \oplus \ldots \oplus R_n, \tag{2.2}$$

où pour $0 \leq i \leq n$, $R_i := e_i(A_K^{\mathcal{M}})$ *est un* $\mathbb{Z}G$*-réseau indécomposable. Aussi*

$$\mathcal{M}A_K = R_0^* \oplus \ldots \oplus R_n^*.$$

(3) *Les réseaux* R_i *sont aussi décrits par*

$$R_i = A_K \cap e_i(K), \quad R_i^* = e_i(A_K).$$

(4) *Pour* $0 \leq i \leq n$, R_i *est un* $\mathbb{Z}G$*-réseau entier, de rang sur* $\mathbb{Z}$ *égal à:* $\varphi(p^i) = p^{i-1}(p-1)$. *Le polynôme caractéristique de l'endomorphisme de* $\mathbb{Q}R_i$ *donné par un générateur de* G *est égal au* p^i*-ème polynôme cyclotomique* $\phi_{p^i}(x)$.

(5) *Pour* $1 \leq i \leq n$, R_i *est pair.*

Démonstration. (1) Il suffit de remarquer que $(\mathcal{M}A_K)^*$ est aussi un $\mathcal{M}$-module et que $(\mathcal{M}A_K)^* \subseteq A_K^* = A_K$; il s'ensuit que $(\mathcal{M}A_K)^* \subseteq A_K^{\mathcal{M}}$ d'où $(A_K^{\mathcal{M}})^* \subseteq \mathcal{M}A_K$; la propriété de minimalité de $\mathcal{M}A_K$ permet de conclure.

(2) De (1.3) on tire la décomposition en modules

$$A_K^{\mathcal{M}} = \bigoplus_i e_i(A_K^{\mathcal{M}}).$$

Il suffit de montrer que les $R_i := e_i(A_K^{\mathcal{M}})$ sont deux à deux orthogonaux: ceci suit du fait que pour $j \neq i$, $\mathrm{Tr}_{K/\mathbb{Q}}(e_i(x), e_j(y)) = \mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j(x), y) = 0$ car $e_i e_j = 0$.

(3) Il est clair que $R_i \subseteq A_K \cap e_i(K)$ et par (2.2) il suffit de montrer que chaque $A_K \cap e_i(K)$ est un $\mathcal{M}$-module: soit x_i dans $A_K \cap e_i(K)$ et soit $m = \sum_j a_j e_j$ dans $\mathcal{M}$ (avec a_j dans $\mathbb{Z}G$); alors $mx_i = a_i x_i$, d'où le résultat car A_K est $\mathbb{Z}G$-stable. Pour R_i^* on procède de façon analogue ou bien on utilise le Lemme 2.4 ci-dessous.

(4) Via les isomorphismes (1.2) on peut considérer R_i et R_i^* comme des sous-$\mathbb{Z}[p^i]$-modules sans torsion dans le $\mathbb{Q}(p^i)$-espace vectoriel $e_i(K)$. Aussi $e_i(K) = \mathbb{Q}R_i$ d'où $\mathrm{rang}_{\mathbb{Z}}(R_i) = \dim_{\mathbb{Q}} e_i(K) = \varphi(p^i)$. Si g est un générateur de G, alors comme $\mathbb{Q}Ge_i \cong \mathbb{Q}(p^i)$ on a $\phi_{p^i}(ge_i) = 0$. Mais $0 = \phi_{p^i}(ge_i) = \phi_{p^i}(g)e_i$ car e_i est un idempotent, d'où $e_i(K) = \ker(\phi_{p^i}(g))$. Comme le degré de $\phi_{p^i}(x)$ est égal à $\varphi(p^i)$, $\phi_{p^i}(x)$ est bien le polynôme caractéristique de g sur $\mathbb{Q}R_i = e_i(K)$.

(5) Le fait que R_i est pair pour $i \geq 1$ est une propriété générale des réseaux ayant un automorphisme de polynôme caractéristique $\phi_{p^i}(x)$ et découle par exemple du Lemme 1-4 de [**1**].

Nous calculons maintenant le discriminant de $A_K^{\mathcal{M}}$, en calculant les discrimants des R_i. Nous allons voir qu'ils ne dépendent que de la ramification sauvage dans $K/\mathbb{Q}$.

Pour le calcul nous introduisons des $\mathbb{Z}G$-réseaux auxiliaires T_i définis par:

$$T_i = A_K \cap \varepsilon_i(K) \quad (0 \leq i \leq n).$$

Soit K_i le sous-corps de K fixe par H_i. Donc $[K_i : \mathbb{Q}] = p^i$, $\varepsilon_i(K) = K_i$ et aussi

$$T_i = A_K \cap K_i.$$

Notons $\mathrm{Tr}_{i,j}$ la forme trace dans l'extension K_i/K_j, ainsi $\mathrm{Tr}_{n,0} = \mathrm{Tr}_{K/\mathbb{Q}}$.

Attention: sauf mention explicite du contraire, la forme sur T_i est toujours $\mathrm{Tr}_{K/\mathbb{Q}}$ et non pas $\mathrm{Tr}_{i,0}$.

PROPOSITION 2.3. (1) *Pour* $0 \leq i \leq n$, T_i *est un* $\mathbb{Z}G$*-réseau de rang* p^i.
(2) *Comme* $\varepsilon_i = e_0 + \ldots + e_i$ *on a les inclusions*

$$T_0 \subseteq T_1 \subseteq \ldots \subseteq T_n = A_K,$$
$$R_0 \oplus \ldots \oplus R_i \subseteq T_i,$$
$$T_{i-1} \oplus R_i \subseteq T_i.$$

(3) *Le dual de* T_i *pour* $\mathrm{Tr}_{K/\mathbb{Q}}$ *est*

$$T_i^* = \varepsilon_i(A_K).$$

(4)
$$\mathrm{disc}(T_i) = \begin{cases} 1 & si \quad n \equiv i \bmod 2, \\ p & sinon, \end{cases}$$
$$\mathrm{disc}(R_0) = \begin{cases} 1 & si \quad n \equiv 0 \bmod 2, \\ p & sinon, \end{cases}$$
$$\mathrm{disc}(R_i) = p \quad pour \quad 1 \leq i \leq n.$$

(5) T_{n-2} *est unimodulaire pour* $\mathrm{Tr}_{n,0}$ *d'après* (4). *La multiplication par p donne une isométrie équivariante entre* $(T_{n-2}, \mathrm{Tr}_{n,0})$ *et* $(A(K_{n-2}/\mathbb{Q}), \mathrm{Tr}_{n-2,0})$.

Démonstration. (1) et (2) sont clairs. Pour montrer (3) nous allons appliquer le lemme suivant à $R = A_K$ et $f = \varepsilon_i$.

LEMME 2.4. *Soit R un réseau dans un* $\mathbb{Q}$*-espace vectoriel V muni d'une forme b et soit f un endomorphisme de V. On définit le transposé* ${}^t f$ *de f en imposant*

$$b(f(x), y) = b(x, {}^t f(y))$$

pour tout x et y de V. Alors $f(R)$ *est un réseau dans* $\mathrm{Im}(f)$ *de dual*

$$(f(R))^* = ({}^t f)^{-1}(R^*) \cap \mathrm{Im}(f).$$

Démonstration du Lemme 2.4. Elle suit des équivalences

$$x \in f(R)^* \quad \Leftrightarrow \quad x \in \mathrm{Im}(f) \text{ et } b(x, f(R)) \subseteq \mathbb{Z},$$
$$b(x, f(R)) \subseteq \mathbb{Z} \quad \Leftrightarrow \quad b({}^t f(x), R) \subseteq \mathbb{Z} \quad \Leftrightarrow \quad x \in ({}^t f)^{-1}(R)^*.$$

La Proposition 2.3(3) suit du lemme car

$$(A_K)^* = A_K \quad \text{et} \quad {}^t\varepsilon_i = \varepsilon_i,$$

d'où $(\varepsilon_i(A_K))^* = (\varepsilon_i^{-1}(A_K)) \cap \varepsilon_i(K) = A_K \cap \varepsilon_i(K) = T_i$ car pour x dans $\varepsilon_i(K)$, $\varepsilon_i(x) = x$.
(4) Par définition:

$$\begin{aligned} \mathrm{disc}(T_i) = [T_i^* : T_i] &= [1/p^{n-i}\,\mathrm{Tr}_{n,i}(A_K) : A_K \cap K_i] \\ &= (N_{i,0}(A_K \cap K_i))/(N_{i,0}(1/p^{n-i}\,\mathrm{Tr}_{n,i}(A_K))) \end{aligned} \tag{2.5}$$

où $N_{i,0}$ est la norme dans $K_i/\mathbb{Q}$.
Rappelons le lemme suivant (voir [**16**, p. 155]).

LEMME 2.6. *Soit J un idéal fractionnaire dans une extension galoisienne K/F, qui soit stable sous l'action de* $\mathrm{Gal}(K/F)$. *Alors*

(a) *J est de la forme* $J = \prod_p \psi(p)^{s(p)}$ *où p parcourt les premiers de F et* $\psi(p)$ *est défini par:* $p\mathbb{Z}_K = (\psi(p))^{e(p)}$;

(b) *si P est un premier divisant p dans K et $\delta = v_p(D(K/F))$, alors*

$$v_p(\mathrm{Tr}_{K/F}(J)) = [(\delta + s)/e]$$

et

$$v_p(J \cap F) = 1 + [(s-1)/e],$$

où $[x]$ dénote le plus grand entier plus petit ou égal à x.

REMARQUE 2.7. Dans ce lemme l'hypothèse que J est stable par $\mathrm{Gal}(K/F)$ est essentielle.

Calculons la valuation de la différente dans notre situation (0.2).

LEMME 2.8. *Soit $K_n/\mathbb{Q}$ une extension sujette aux conditions* (0.2) *et soit K_i le sous-corps de K_n tel que $[K_i : \mathbb{Q}] = p^i$. Pour $0 \leqslant i \leqslant n$, notons: $P(i)$ l'unique idéal premier de K_i au-dessus de p, et δ_i (respectivement $\delta_{i,j}$) la valuation en $P(i)$ de la différente de $K_i/\mathbb{Q}$ (respectivement K_i/K_j). Alors*

(1) $\delta_i = (i+1)p^i - 2 - (p^i - p)/(p-1)$,

(2) $\delta_{i,j} = \delta_i - p^{i-j}\delta_j$.

Le lemme suit d'un calcul standard utilisant la formule (1.8) et de la propriété de transitivité de la différente.

Valuation en $q \neq p$ de $\mathrm{disc}(T_i)$. Tout premier $q \neq p$ se ramifie modérément dans $K = K_n/\mathbb{Q}$, donc la valuation d de la différente $D(K/\mathbb{Q})$ en $\psi(q)$ est $d = e - 1$ (voir Lemme 2.6 pour les notations). D'où il suit—par définition de A_K—que la valuation de A_K en $\psi(q)$ est $-\frac{1}{2}(e-1)$. Du Lemme 2.6, on tire alors pour Q au-dessus de q:

$$v_Q(\mathrm{Tr}_{n,i}(A_K)) = v_Q(A_K \cap K_i).$$

Par conséquent $q \neq p$ ne divise pas $\mathrm{disc}(T_i)$.

Valuation en p de $\mathrm{disc}(T_i)$. D'après (2.5), et comme p se ramifie totalement dans $K/\mathbb{Q}$, on a

$$v_p(\mathrm{disc}(T_i)) = p^i(n-i) + v_{P(i)}(A_K \cap K_i) - v_{P(i)}(\mathrm{Tr}_{n,i}(A_K)).$$

Par le Lemme 2.8, $\delta_{n,i} = \delta_n - p^{n-i}\delta_i$. Par définition $v_{P(n)}(A_K) = -\frac{1}{2}\delta_n$ et l'indice de ramification de $P(i)$ dans K/K_i est $e_{n,i} = p^{n-i}$. Donc le Lemme 2.6 entraîne que

$$v_p(\mathrm{disc}(T_i)) = p^i(n-i) + \delta_i - 2[\delta_n/2p^{n-i}] \tag{2.9}$$

et de l'expression pour δ_n du Lemme 2.8 on obtient alors

$$[\delta_n/2p^{n-i}] = \begin{cases} \frac{1}{2}((n+1)p^i - (p^i-p)/(p-1)) - 1 & \text{si } n \equiv i \bmod 2, \\ \frac{1}{2}((n+1)p^i - (p^i-1)/(p-1)) - 1 & \text{sinon.} \end{cases}$$

En remplaçant dans (2.9) on obtient le résultat voulu.

Calcul de $\mathrm{disc}(R_i)$. On a vu à la Proposition 2.3(2) que

$$T_{i-1} \oplus R_i \subseteq T_i \subseteq T_i^* \subseteq T_{i-1}^* \oplus R_i^*,$$

donc $\mathrm{disc}(T_{i-1})\mathrm{disc}(R_i) = [T_i : T_{i-1} \oplus R_i]^2 \mathrm{disc}(T_i)$ et il suffit de montrer

$$[T_i : T_{i-1} \oplus R_i] = \mathrm{disc}(T_{i-1}), \tag{2.10}$$

car alors $\mathrm{disc}(R_i) = \mathrm{disc}(T_i)\mathrm{disc}(T_{i-1}) = p$. Pour $i = 0$ on a $e_0 = \varepsilon_0$ donc $R_0 = T_0$. Pour $i \geq 1$ montrons

$$T_i/(T_{i-1} \oplus R_i) \cong T_{i-1}^*/T_{i-1}.$$

Soit f l'application de T_i dans T_{i-1}^*/T_{i-1}, telle que $f(x) = \varepsilon_i(x) \bmod T_{i-1}$. Alors f est surjective car: si T_i est unimodulaire alors $\varepsilon_{i-1}(T_i)$ est le dual de $T_i \cap \varepsilon_{i-1}(K) = A_K \cap K_{i-1} = T_{i-1}$ et si $T_i \neq T_i^*$ alors $T_{i-1} = T_{i-1}^*$. Calculons le noyau de f: pour x dans T_i, comme $x = \varepsilon_i(x) = \varepsilon_{i-1}(x) + \varepsilon_i(x)$, on a les équivalences

$$\varepsilon_{i-1}(x) \in T_{i-1} \quad \Leftrightarrow \quad e_i(x) \in R_i \quad \Leftrightarrow \quad x \in T_{i-1} \oplus R_i.$$

Ainsi (2.10) est démontré.

(5) T_{n-2} est unimodulaire pour $\mathrm{Tr}_{n,0}$ par le point (4), donc pT_{n-2} est unimodulaire pour $\mathrm{Tr}_{n-2,0}$ car si x est dans K_{n-2} alors $\mathrm{Tr}_{n,0}(x) = p^2\mathrm{Tr}_{n-2,0}(x)$. Comme pT_{n-2} est un idéal, il est égal à $A(K_{n-2}/\mathbb{Q})$.

Ceci achève la démonstration de la Proposition 2.3.

REMARQUE 2.11. Les R_i ont un discriminant minimal, dans le sens où un réseau quelconque ayant les propriétés de R_i énoncées à la Proposition 2.1(4) a pour discriminant un multiple de p (voir § 4, Remarque 4.5). En particulier pour $i \geq 1$ les R_i ne pouvaient pas être unimodulaires.

3. *Réduction à la détermination des réseaux R_i et R_i^**

On garde les notations précédentes; en particulier $K/\mathbb{Q}$ satisfait aux conditions (0.2), K_i est l'unique sous-corps de $K = K_n$ de degré p^i sur $\mathbb{Q}$ et $\mathrm{Tr}_{i,j}$ dénote la trace dans K_i/K_j. Les réseaux R_i et R_i^* ont été définis au paragraphe précédent (voir Proposition 2.1).

THÉORÈME 3.1. *Si $n \geq 2$ on a une $\mathbb{Z}G$-isométrie*

$$(A_K, \mathrm{Tr}_{K/\mathbb{Q}}) \sim (A(K_{n-2}/\mathbb{Q}), \mathrm{Tr}_{n-2,0}) \oplus (B_n, \mathrm{Tr}_{K/\mathbb{Q}})$$

où $(B_n, \mathrm{Tr}_{K/\mathbb{Q}})$ est un $\mathbb{Z}G$-réseau unimodulaire de rang $p^n - p^{n-2}$. On pose $B_1 = A(K_1/\mathbb{Q})$. Alors pour tout $n \geq 1$,

$$R_{n-1} \oplus R_n \subseteq B_n$$

et la classe d'isométrie équivariante de B_n est déterminée par celles de R_{n-1} et R_n.

A la Proposition 6.6 nous donnerons une décomposition de A_K en termes des réseaux B_i.

Il est clair que, par récurrence sur n, le Théorème 0.3 suit du Théorème 3.1 une fois que l'on aura montré—au § 5—que la classe d'isométrie des R_i et R_i^* ne dépend que des conditions (0.2).

Démonstration. Nous savons par la Proposition 2.3 que pour tout n le $\mathbb{Z}G$-réseau $(T_{n-2}, \mathrm{Tr}_{K/\mathbb{Q}})$ est unimodulaire: rappelons que $T_{n-2} := A_K \cap K_{n-2}$. D'après un lemme connu [**12**, 1.3.1] l'inclusion $T_{n-2} \subseteq A_K$ donne la décomposition en $\mathbb{Z}G$-réseaux

$$(A_K, \mathrm{Tr}_{K/\mathbb{Q}}) \sim (T_{n-2}, \mathrm{Tr}_{K/\mathbb{Q}}) \oplus (B_n, \mathrm{Tr}_{K/\mathbb{Q}})$$

où B_n est le complément orthogonal de T_{n-2} dans A_K formé des éléments x de A_K tels que $\mathrm{Tr}_{K/\mathbb{Q}}(xT_{n-2}) = 0$. La Proposition 2.3(5) donne l'isométrie

$$(T_{n-2}, \mathrm{Tr}_{K/\mathbb{Q}}) \sim (A(K_{n-2}/\mathbb{Q}), \mathrm{Tr}_{n-2,0})$$

et il ne nous reste qu'à montrer que B_n a les propriétés voulues.

Remarquons que B_n est unimodulaire puisque A_K et T_{n-2} le sont. Comme $R_{n-1} \oplus R_n$ est inclus dans l'orthogonal de K_{n-2} (pour $\mathrm{Tr}_{K/\mathbb{Q}}$) on a bien

$$R_{n-1} \oplus R_n \subseteq B_n = B_n^* \subseteq R_{n-1}^* \oplus R_n^*. \tag{3.2}$$

Montrons qu'à $\mathbb{Z}G$-isométrie près il y a un seul réseau B_n vérifiant ces inclusions. Pour tout $i \geq 1$, $\mathrm{disc}(R_i) = p$ donc $R_i^*/R_i \cong \mathbb{F}_p$. La forme $\mathrm{Tr}_{K/\mathbb{Q}}$ induit sur ce quotient une forme non-nulle que nous noterons

$$b_i\colon\ R_i^*/R_i \times R_i^*/R_i \to (1/p)\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}.$$

Les réseaux B unimodulaires vérifiant les inclusions (3.2) correspondent bijectivement aux droites isotropes du quotient $(R_{n-1}^* \oplus R_n^*)/(R_{n-1} \oplus R_n) \cong \mathbb{F}_p \oplus \mathbb{F}_p$ muni de la forme $b = b_{n-1} \oplus b_n$.

LEMME 3.3. *$\mathbb{F}_p \oplus \mathbb{F}_p$ muni de b possède exactement deux droites isotropes. Les réseaux B et B' correspondants sont $\mathbb{Z}G$-isométriques.*

Démonstration du lemme. (Voir aussi [**9**].) Soit $x_0 \neq 0$ dans $\mathbb{F}_p \oplus \{0\}$ et $y_0 \neq 0$ dans $\{0\} \oplus \mathbb{F}_p$. Comme $b(x_0) \neq 0$, une droite isotrope contient forcément un vecteur de la forme $x_0 + ky_0$ avec k dans $\mathbb{F}_p \backslash \{0\}$ et tel que

$$b_{n-1}(x_0) + k^2 b_n(y_0) = 0.$$

Ceci donne deux choix opposés pour k, d'où deux droites. (On a au moins une solution car B_n existe!). La $\mathbb{Z}G$-isométrie de $R_{n-1}^* \oplus R_n^*$ qui envoye (x, y) sur $(x, -y)$ passe au quotient et échange les deux droites isotropes, donc aussi les deux réseaux B et B' correspondants.

4. *Classification de formes sur les corps cyclotomiques $\mathbb{Q}(p^i)$*

Notations du paragraphe. Dans ce paragraphe on fixe l'entier $i \geq 1$ et on pose

$k = \mathbb{Q}(p^i)$, $k^+ = \mathbb{Q}(p^i) \cap \mathbb{R}$,

μ: groupe des racines p^i-èmes de l'unité dans k,

ζ: un générateur de μ,

$\bar{}$: conjugaison complexe,

$\mathcal{P} = (1-\zeta)\mathbb{Z}_k$, $\beta = (1-\zeta)(1-\bar{\zeta})$,

$P = \mathcal{P}\bar{\mathcal{P}} \cap k^+ = \beta\mathbb{Z}_{k^+}$, $m(i) = -\frac{1}{2}(p^{i-1}+1)$,

$\delta = p^i \beta^{m(i)}$, $\mathrm{tr} = \mathrm{trace}_{k/\mathbb{Q}}$.

Remarquons que δ est un générateur totalement positif de la différente de l'extension $k^+/\mathbb{Q}$ [**17**, chapitre 2].

Rappelons que nous cherchons maintenant à déterminer la classe de $\mathbb{Z}G$-isométrie de R_i (pour tout $i \geq 1$). Le choix d'une racine de l'unité d'ordre p^i permet de voir R_i comme un $\mathbb{Z}_k$-module (Proposition 2.1(4)). Etant de rang 1 sur

$\mathbb{Z}_k$, R_i est isomorphe à un idéal de k qui—par cet isomorphisme—est muni d'une forme satisfaisant les propriétés suivantes: cette forme est

$$\begin{array}{l} \textit{entière,} \\ \textit{invariante sous l'action de } \mu, \\ \textit{définie positive,} \\ \textit{de discriminant } p \end{array} \tag{4.1}$$

(voir Propositions 2.1 et 2.3). Nous allons décrire les formes ayant ces propriétés. On appellera $\mathbb{Z}_k$-réseau un $\mathbb{Z}_k$-module muni d'une forme invariante sous μ.

PROPOSITION 4.2. (1) *A une forme bilinéaire symétrique* b: $k \times k \to \mathbb{Q}$ *invariante par* μ *on associe un unique* α *dans* k^+ *tel que* $b(x, y) = \mathrm{tr}(\alpha x \bar{y})$. *On pose* $a = \alpha\delta$.

(2) b *est définie positive si et seulement si* a *est totalement positif, i.e. tous les conjugués de* a *sont positifs.*

(3) *On note* (J, a) *le* $\mathbb{Z}_k$*-réseau obtenu en munissant l'idéal* J *de* k *de la forme*

$$b(x, y) = \mathrm{tr}(\alpha x \bar{y}) \quad \textit{avec} \quad a = \alpha\delta.$$

Alors (J, a) *est entier de discriminant* p *si et seulement si* $aJ\bar{J} = \mathbb{Z}_k$.

(4) *Les réseaux* (J, a) *et* (J', a') *sont* $\mathbb{Z}_k$*-isométriques si et seulement si il existe* λ *dans* k *avec* $J' = \lambda J$ *et* $a = \lambda\bar{\lambda}a'$.

Démonstration. (Voir aussi [**13**] et [**9**].) (1) Pour tout y dans k l'application qui à x associe $b(x, y)$ est une forme $\mathbb{Q}$-linéaire donc, comme la forme trace tr est non-dégénérée, il existe un unique $h(y)$ tel que pour tout x et y dans k,

$$b(x, y) = \mathrm{tr}(xh(y)).$$

Comme b est invariante par μ et que les puissances de ζ forment une $\mathbb{Q}$-base pour k on a pour tout y' dans k,

$$b(y'x, y) = b(x, \bar{y}'y)$$

d'où

$$\mathrm{tr}(y'xh(y)) = \mathrm{tr}(xh(\bar{y}'y))$$

et donc pour tout y et y' dans k, $y'h(y) = h(\bar{y}'y)$. Soit $\alpha := h(1)$; alors $\alpha = \bar{\alpha}$ est bien dans k^+ par symétrie de b et on a le résultat voulu.

(2) De façon générale la signature de la forme $\mathrm{tr}(\alpha x\bar{y})$ est égale à

$$\mathrm{Card}\{\sigma \in \mathrm{Gal}(k/\mathbb{Q}) \mid \sigma(\alpha) > 0\} - \mathrm{Card}\{\sigma \in \mathrm{Gal}(k/\mathbb{Q}) \mid \sigma(\alpha) < 0\}.$$

(3) Calculons le dual de (J, a):

$$x \in J^* \quad \Leftrightarrow \quad \mathrm{tr}(\alpha x\bar{J}) \subseteq \mathbb{Z} \quad \Leftrightarrow \quad x \in (\alpha\bar{J}D(k/\mathbb{Q}))^{-1}.$$

Donc

$$J^* = (\alpha\bar{J}D(k/\mathbb{Q}))^{-1} = (a(1-\zeta)\bar{J})^{-1} \tag{4.3}$$

par la transitivité de la différente, la définition de δ et le fait que $D(k/k^+) = (1-\zeta)\mathbb{Z}_k$.

Le réseau (J, a) est entier si et seulement si $J \subseteq J^*$, ce qui équivaut par (4.3) à $aJ\bar{J} \subseteq (1-\zeta)^{-1}\mathbb{Z}_k$; mais comme $P = \bar{P}$ et $a \in k^+$, la valuation en P de $aJ\bar{J}$ est

paire et

$$aJ\bar{J} \subseteq (1-\zeta)^{-1}\mathbb{Z}_k \quad \Leftrightarrow \quad aJ\bar{J} \subseteq \mathbb{Z}_k.$$

Si (J, a) est entier,

$$\begin{aligned} \operatorname{disc}(J) &= N_{k/\mathbb{Q}}(J)N_{k/\mathbb{Q}}(a\bar{J})N_{k/\mathbb{Q}}(1-\zeta) \\ &= p[a^{-1}\bar{J}^{-1} : J]. \end{aligned} \tag{4.4}$$

Donc le discriminant de (J, a) est p si et seulement si $a^{-1}\bar{J}^{-1} = J$, c'est-à-dire $aJ\bar{J} = \mathbb{Z}_k$.

(4) Une $\mathbb{Z}_k$-isométrie entre (J, a) et (J', a') est d'abord un isomorphisme de $\mathbb{Z}_k$-modules, donc une homothétie de rapport un λ dans k. Ceci impose $J' = \lambda J$. Ecrivons que cette homothétie est une isométrie: pour tout x, y dans J et avec $a = \alpha\delta$ et $a' = \beta\delta$,

$$\operatorname{tr}(\beta(\lambda x)(\bar{\lambda}\bar{y})) = \operatorname{tr}(\alpha x\bar{y}),$$

soit $a'\lambda\bar{\lambda} = a$.

REMARQUE 4.5. L'égalité (4.4) montre que le discriminant de (J, a) est nécessairement un multiple de p.

La proposition précédente permet de décrire l'ensemble $Q(J)$ des classes de $\mathbb{Z}_k$-isométrie de $\mathbb{Z}_k$-formes sur un idéal J fixé ayant les propriétés (4.1).

Soit $\mathrm{Cl}(k)$ le groupe des classes d'idéaux de k et $\mathrm{Cl}(k^+)^+$ le groupe des classes d'idéaux au sens restreint de k^+. Soit N^+ le noyau de la norme de $\mathrm{Cl}(k)$ dans $\mathrm{Cl}(k^+)^+$. Alors N^+ est le sous-groupe de $\mathrm{Cl}(k)$ formé des classes d'idéaux $[J]$ telles que $J\bar{J}$ soit principal et engendré par un élément totalement positif.

Soit E^{++} le groupe des unités totalement positives de k^+ et soit E^{**} le groupe des normes d'unités de k, qui est aussi le groupe des carrés d'unités de k^+: E^{**} est inclus dans E^{++} et nous posons

$$\mathscr{C} = E^{++}/E^{**}.$$

COROLLAIRE 4.6. *Soit fixé un idéal J de k dont la classe $[J]$ appartient à N^+. Soit a un élément totalement positif de k^+ tel que*

$$aJ\bar{J} = \mathbb{Z}_k.$$

L'application qui à (J', a') associe $a'a^{-1}$ est une bijection de l'ensemble $Q(J)$ sur le groupe $\mathscr{C}$.

COROLLAIRE 4.7. *Le nombre de classes de $\mathbb{Z}_k$-isométrie de $\mathbb{Z}_k$-réseaux entiers de rang 1, de discriminant p, et définis positifs est*

$$c = \mathrm{Card}(N^+)[E^{++} : E^{**}].$$

REMARQUE 4.8. Jacques Martinet a observé que le nombre c du Corollaire 4.7 est égal au quotient du nombre de classes de k par le nombre de classes de k^+.

5. *Structure galoisienne et forme trace*

THÉORÈME 5.1. *Soit $K/\mathbb{Q}$ une extension galoisienne soumise au seules conditions* (0.2). *Alors pour $i \geq 1$, $(R_i, \mathrm{Tr}_{K/\mathbb{Q}})$ est $\mathbb{Z}G$-isométrique à $(\mathbb{Z}[p^i], 1)$.*

Pour la démonstration de ce théorème nous allons utiliser deux résultats démontrés dans [8]. Le premier est que pour une extension $K/\mathbb{Q}$ satisfaisant (0.2), $\mathcal{M}A_K$ est libre en tant que $\mathcal{M}$-module. Le deuxième est le calcul des valuations de certaines résolvantes liées à A_K.

REMARQUE 5.2. [8] traite de la structure de $\mathcal{M}A_K$ en toute généralité avec comme seule condition la projectivité de A_K en tant que $\mathbb{Z}G$-module. Bien que A_K ne soit pas projectif ici, on peut néanmoins appliquer les résultats de [8], car dans la situation qui est la notre, la classe de $\mathcal{M}A_K$ dans $\mathrm{Cl}(\mathcal{M})$ ne dépend que de la ramification modérée: en effet les idéaux au-dessus de p dans les corps cyclotomiques $\mathbb{Q}(p^i)$ sont principaux (regarder (1.4)).

Par ce qui vient d'être dit, il existe a dans $\mathcal{M}A_K$ tel que $\mathcal{M}A_K = \mathcal{M}a$. En étendant à K on obtient $K = \mathbb{Q}Ga$ et cette égalité donne l'isomorphisme

$$\varphi\colon\ K = \mathbb{Q}Ga \cong \mathbb{Q}G, \quad \varphi(\lambda a) = \lambda.$$

Si K est muni de la forme $\mathrm{Tr}_{K/\mathbb{Q}}$, on transforme φ en isométrie en mettant sur $\mathbb{Q}G$ la forme

$$T_{s(a)}\colon\ \mathbb{Q}G \times \mathbb{Q}G \to \mathbb{Q}, \quad T_{s(a)}(x, y) = \mathrm{pr}_1(s(a)x\bar{y})$$

où les notations sont celles de l'Exemple 1.5 et $s(a)$ est l'élément de $\mathbb{Q}G$ défini par

$$s(a) = \sum_G \mathrm{Tr}_{K/\mathbb{Q}}(ag(a))g^{-1}.$$

D'après l'Exemple 1.5 et avec les notations du § 4 on obtient la

PROPOSITION 5.3. *Soit $\psi = \bigoplus_i \chi_i$ l'isomorphisme entre $\mathbb{Q}G$ et $\bigoplus_i \mathbb{Q}(p^i)$ de* (1.2). *Alors pour tout $i \geq 1$ la restriction de $\psi \circ \varphi$ à R_i^* est une $\mathbb{Z}G$-isométrie de $(R_i^*, \mathrm{Tr}_{K/\mathbb{Q}})$ sur $(\mathbb{Z}[p^i], \sigma_i |G|^{-1}\delta_i)$ où $\sigma_i = \chi_i(s(a))$. En dualisant on obtient que $(R_i, \mathrm{Tr}_{K/\mathbb{Q}})$ est isométrique à $(\mathbb{Z}[p^i], |G|(\sigma_i\delta_i\beta_i)^{-1})$.*

En effet par la Proposition 2.1(3), $R_i^* = e_i(A_K) = \mathbb{Z}Ge_i(a)$, donc $\psi \circ \varphi(R_i^*) = \psi(\mathbb{Z}Ge_i) = \mathbb{Z}[p^i]$. Pour calculer le dual de $(\mathbb{Z}[p^i], \sigma_i^{-1}|G|\beta_i^{-1})$ utiliser (4.3) et le fait que $s(a) = \bar{s}(a)$.

Pour démontrer le Théorème 5.1 il suffit donc de vérifier, d'après le Corollaire 4.6, que l'élément $E_i = |G|(\sigma_i\delta_i\beta_i)^{-1}$ est trivial dans le groupe $\mathscr{E}$, c'est-à-dire que E_i, qui est une unité de k_i^+, est la norme d'une unité de k_i.

Nous allons décrire l'élément σ_i en termes de résolvantes. Soit χ un caractère de G et

$$(a \mid \chi) = \sum_G \chi(g^{-1})g(a)$$

la résolvante de a par rapport à χ.

LEMME 5.4. *Dans $\mathbb{Q}(p^i)$ on a l'égalité*

$$\sigma_i = (a \mid \chi_i)\overline{(a \mid \chi_i)}.$$

Remarquons que $(a \mid \chi_i)\overline{(a \mid \chi_i)}$ est un élément de k_i, et même de k_i^+, alors que $(a \mid \chi_i)$ lui est dans Kk_i.

Le lemme découle de l'égalité suivante en appliquant χ_i:

$$\Big(\sum_G h(a)h^{-1}\Big)\Big(\sum_G g(a)g\Big) = \sum_{G\times G} h(a)g(a)gh^{-1}$$
$$= \sum_{G\times G} g(a)gk^{-1}(a)k$$
$$= \sum_G \mathrm{Tr}_{K/\mathbb{Q}}(ah(a))h^{-1}.$$

Ensuite nous utilisons les résultats de [**8**] qui entraînent que

$$(a \mid \chi_i)(\tau(\chi_i^2)\tau(\chi_i)^{-1})^{-1}$$

est dans k_i et engendre une puissance de l'idéal $(1-\zeta_i)\mathbb{Z}[p^i]$. Ici $\tau(\chi)$ est la somme de Gauss associée à la partie modérée du caractère χ et χ^2 est le caractère de valeurs $\chi^2(g) := \chi(g^2)$. On sait que si on pose

$$f(\chi) = \tau(\chi)\bar{\tau}(\chi) \quad \text{(le conducteur)}$$

alors, comme $|G|$ est impair, χ^2 est conjugué de χ et on a $f(\chi^2) = f(\chi)$, donc

$$\tau(\chi_i^2)\tau(\chi_i)^{-1}\bar{\tau}(\chi_i^2)\bar{\tau}(\chi_i)^{-1} = 1.$$

On en déduit qu'il existe u_i dans E_{k_i} et $n(i)$ un entier relatif tels que $(a \mid \chi_i) = u_i(1-\zeta_i)^{n(i)}$ et donc

$$\sigma_i = (a \mid \chi_i)\overline{(a \mid \chi_i)} = u_i\bar{u}_i\beta_i^{n(i)}.$$

En revenant à E_i,

$$E_i = (u_i\bar{u}_i)^{-1}p^{n-i}\beta_i((p^{i-1}-1)/2) - n(i)$$

mais E_i est une unité donc

$$\tfrac{1}{2}(n-i)(p^i - p^{i-1}) + \tfrac{1}{2}(p^{i-1}-1) - n(i) = 0$$

et

$$E_i = (p\beta_i^{t(i)})^{n-i} \quad \text{modulo } N(E_{k_i})$$

où $t(i) = -\frac{1}{2}(p^i - p^{i-1})$. Il reste à vérifier que $B := p\beta_i^{t(i)}$ est dans $N(E_{k_i})$. Mais $p = N_{k_i^+/\mathbb{Q}}(\beta_i)$ donc $B = \prod_\sigma \sigma(\beta_i)\beta_i^{-1}$, où σ parcourt $\mathrm{Gal}(k_i^+/\mathbb{Q})$. Si on note encore σ un prolongement de σ à k_i,

$$\sigma(\beta_i)\beta_i^{-1} = [(1-\sigma(\zeta_i))(1-\zeta_i)^{-1}]\overline{[(1-\sigma(\zeta_i))(1-\zeta_i)^{-1}]}.$$

Donc $E_i = 1$ modulo $N(E_{k_i})$ et (5.1) est démontré.

REMARQUE 5.5. Le résultat de (5.1) est indépendant du choix initial des caractères χ_i, ce qui prouve bien que les réseaux A_K de deux extensions vérifiant (0.2) sont $\mathbb{Z}G$-isométriques, pour toute identification de leurs groupes de Galois.

REMARQUE 5.6. Avec les méthodes de ce paragraphe et les résultats de [**10**] on peut retrouver—de façon plus directe mais équivalente—le fait que dans une extension cyclique $K/\mathbb{Q}$ de degré premier $p \neq 2$ le discriminant de l'extension classe le réseau $(\mathbb{Z}_K, \mathrm{Tr}_{K/\mathbb{Q}})$ à isométrie équivariante près (voir [**4**, Chapter IV]). Ceci sans hypothèse de ramification. Au lieu des résultats de [**8**] on utilise le Théorème 7 de [**10**] qui exprime le produit $(a \mid \chi)\overline{(a \mid \chi)}$ des résolvantes associées à $\mathbb{Z}_K$ en termes du conducteur de χ.

6. *Description explicite de A_K: systèmes de racines*

Notations du paragraphe. Pour chaque i on reprend les notations du § 4. Si $j \leqslant i$ on pose

$$\zeta_j = (\zeta_i)^{p^{i-j}}.$$

La forme $\mathrm{tr}_{i,0}(\delta_i^{-1} x\bar{y})$ sur $(\mathbb{Z}[p^i], 1)$ sera notée $b_i(x, y)$.

6.1. *Propriétés de $(\mathbb{Z}[p^i], 1)$ pour $i \geqslant 1$*

Pour tout entier $q \geqslant 1$ il existe un unique réseau entier défini positif $(\mathbb{A}_q, b)$ de rang q, de discriminant $q+1$ et ayant une base formée de *racines*, i.e. de vecteurs x avec $b(x, x) = 2$. Soit $\{e_i\}$ la base canonique de $\mathbb{R}^{q+1}$. On peut voir $\mathbb{A}_q$ plongé dans l'espace euclidien $\mathbb{R}^{q+1}$ muni de la forme standard $\langle 1, \ldots, 1\rangle$; une base de $\mathbb{A}_q$ est donnée par les q vecteurs

$$a_i = e_{i+1} - e_i \quad (1 \leqslant i \leqslant q). \tag{6.1}$$

On définit le *système de racines* d'un réseau entier (pair, défini positif) (R, b) comme étant le sous-réseau engendré par ses vecteurs x avec $b(x, x) = 2$. On le note $\mathrm{Rac}(R, b)$. Rappelons le théorème de structure suivant.

PROPOSITION 6.2 (Witt) [**3**, chapitre VI, No. 4.2]. *Un réseau entier, défini positif (R, b) qui est engendré par des vecteurs e_i avec $b(e_i, e_i) = 2$ est une somme orthogonale de systèmes de racines*

$$\mathbb{A}_q, \mathbb{D}_q, \mathbb{E}_6, \mathbb{E}_7, \mathbb{E}_8.$$

Les indices indiquent les rangs respectifs et les discriminants sont

$$\mathrm{disc}(\mathbb{A}_q) = q+1, \quad \mathrm{disc}(\mathbb{E}_6) = 3, \quad \mathrm{disc}(\mathbb{E}_8) = 1,$$
$$\mathrm{disc}(\mathbb{D}_q) = 4, \qquad \mathrm{disc}(\mathbb{E}_7) = 2.$$

Dans la suite, seule la famille des $\mathbb{A}_q$ interviendra directement (cependant il y a une exception pour $p = 3$). Nous renvoyons à [**5**, Chapter 4] pour les définitions des autres systèmes de racines irréductibles ainsi que pour une discussion des propriétés de ces réseaux.

PROPOSITION 6.3. *$(i = 1)$ $(\mathbb{Z}[p], 1)$ est isométrique à $\mathbb{A}_{p-1}$.*

Démonstration. Un calcul facile montre que dans la base $\{1, \zeta_i, \ldots, \zeta_i^{p-2}\}$ la matrice de la forme b_1 est bien celle donnée par la base (6.1) avec $q = p-1$.

PROPOSITION 6.4. *Pour $0 < j < i$, $(\mathbb{Z}[p^i], 1)$ contient la somme orthogonale de p^{i-j} copies de $(\mathbb{Z}[p^j], 1)$.*

Démonstration. On définit une unité u_{ij} de $\mathbb{Z}[p^i]$ par

$$u_{ij} = (1 - \zeta_j)(1 - \zeta_i)^{-p^{i-j}}.$$

Alors l'application f_{ij} de $\mathbb{Z}[p^j]$ dans $\mathbb{Z}[p^i]$ définie par

$$f_{ij}(x) = x(1 - \zeta_i)^{(p^{i-j}-1)/2} u_{ij}^{(p^{j-1}+1)/2}$$

est une isométrie de $(\mathbb{Z}[p^j], b_j)$ sur un sous réseau Z_j de $(\mathbb{Z}[p^i], b_i)$. La somme orthogonale des p^{i-j} translatés différents de Z_j par l'itération de la multiplication par ζ_i est le réseau cherché.

NOTATION. On désigne par $n(R)$ la somme orthogonale de n copies du réseau R.

PROPOSITION 6.5. *Pour $p \neq 3$ et pour $i \geq 1$, ainsi que pour $p = 3$ et $i = 1$:*

$$\mathrm{Rac}(\mathbb{Z}[p^i], 1) = (p^{i-1})(\mathbb{A}_{p-1}).$$

Pour $p = 3$ et $i \geq 2$:

$$\mathrm{Rac}(\mathbb{Z}[3^i], 1) = (3^{i-2})(\mathbb{E}_6).$$

Démonstration. Par la Proposition 6.2 on sait que $\mathrm{Rac} = \mathrm{Rac}(\mathbb{Z}[p^i], 1)$ est une somme orthogonale de réseaux $\mathbb{A}_q$, $\mathbb{D}_q$, $\mathbb{E}_6$, $\mathbb{E}_7$ ou $\mathbb{E}_8$. Comme $\mathbb{Z}[p^i]$ est indécomposable en tant que $\mathbb{Z}[p^i]$-module il ne peut apparaître dans cette somme qu'un seul type de réseau. Les Propositions 6.3 et 6.4 prouvent que

$$(p^{i-1})(\mathbb{A}_{p-1}) \subseteq \mathrm{Rac} \subseteq (\mathbb{Z}[p^i], 1),$$

donc Rac est de rang $p^i - p^{i-1}$ et de discriminant une puissance de p. En vue des propriétés des réseaux de la Proposition 6.2, il suit facilement que pour $p \neq 3$ la seule possibilité est bien $\mathrm{Rac} = (p^{i-1})(\mathbb{A}_{p-1})$. Cette analyse donne par contre deux possibilités si $p = 3$ et $i \geq 2$: $(3^{i-1})(\mathbb{A}_2)$ et $(3^{i-2})(\mathbb{E}_6)$. Mais la Proposition 6.4 appliquée avec $j = 2$ montre que

$$(3^{i-2})(\mathbb{Z}[9], 1) \subseteq (\mathbb{Z}[3^i], 1).$$

Or $(\mathbb{Z}[9], 1)$ est un réseau pair de rang 6, discriminant 3 et défini positif; le seul réseau ayant ces propriétés est $\mathbb{E}_6$ (voir [5, Table 15-9]). Ceci termine la démonstration.

6.2. *Décomposition de A_K*

Soit $K/\mathbb{Q}$ une extension soumise aux seules conditions (0.2).

PROPOSITION 6.6. *Suivant la parité de n, on a les $\mathbb{Z}G$-isométries*

$$A_K \sim \langle 1 \rangle \oplus B_2 \oplus B_4 \oplus \ldots \oplus B_n, \quad \text{si } n \text{ est pair}$$

ou

$$A_K \sim B_1 \oplus B_3 \oplus \ldots \oplus B_n, \quad \text{si } n \text{ est impair.}$$

Ici, pour $i \geq 2$, $B_i = B_i(p)$ est l'unique réseau unimodulaire contenant un sous-réseau d'indice p $\mathbb{Z}G$-isométrique à

$$(\mathbb{Z}[p^{i-1}], 1) \oplus (\mathbb{Z}[p^i], 1)$$

et pour $i = 1$,

$$B_1 \sim \langle 1, \ldots, 1 \rangle. \tag{6.7}$$

Démonstration. Elle découle des Théorèmes 3.1 et 5.1. Pour (6.7) remarquons que nous savons par (3.1) que $R_0 \oplus R_1 \subseteq B_1$, c'est-à-dire $\langle p \rangle \oplus \mathbb{A}_{p-1} \subseteq B_1$ (d'après (6.3)), de plus le Lemme 3.3 montre que ceci caracterise B_1 à isométrie près. L'isométrie (6.7) suit alors du fait que $\mathbb{A}_{p-1}$ peut être construit comme le complément orthogonal d'un vecteur de longueur p dans $\mathbb{Z}^p$ muni de la forme standard $\langle 1, \ldots, 1 \rangle$ (voir [5, Chapter 4.6]).

REMARQUE 6.8. L'isométrie (6.7) donne une autre démonstration du fait que, si $K/\mathbb{Q}$ est cyclique de degré p, alors $(A_K, \mathrm{Tr}_{K/\mathbb{Q}})$ est $\mathbb{Z}G$-isométrique à $(\mathbb{Z}G, T_1)$ (voir [7]).

PROPOSITION 6.9. *Pour $i \geqslant 2$ les B_i sont des $\mathbb{Z}G$-réseaux $\mathbb{Z}$-indécomposables. Leur système de racines est:*

$$\begin{aligned} &(p^{i-2}+p^{i-1})(\mathbb{A}_{p-1}) && \text{pour } p \neq 3, \\ &(p^{i-3}+p^{i-2})(\mathbb{E}_6) && \text{pour } p = 3 \text{ et } i \geqslant 3, \\ &\mathbb{E}_8 && \text{pour } p = 3 \text{ et } i = 2. \end{aligned}$$

Démonstration. Le $\mathbb{Q}G$-module $\mathbb{Q}B_i$ est isomorphe à $\mathbb{Q}(p^{i-1}) \oplus \mathbb{Q}(p^i)$ donc la seule décomposition non-triviale de B_i en somme de $\mathbb{Z}G$-réseaux aurait la forme $B_i = M \oplus N$ où M (respectivement N) serait un $\mathbb{Z}[p^{i-1}]$ (respectivement $\mathbb{Z}[p^i]$)-réseau. On a remarqué au point (4.5) que de tels réseaux ont pour discriminant un multiple de p; donc une telle décomposition contredirait le fait que B_i est unimodulaire. Donc, si B_i est $\mathbb{Z}$-décomposable, la seule possibilité est qu'il soit isotypique, i.e. $B_i = (p^u)L$ pour un certain réseau L et $u \leqslant i-2$. Dans cette décomposition les copies de L sont permutées circulairement sous l'action d'un générateur g de G. Elles sont toutefois stables par e_i car e_i est un polynôme en $g^{p^{i-1}}$, donc en g^{p^u}. On en tire que $R_i = e_i(B_i) = e_i(L)^{p^u}$ et $\operatorname{disc}(R_i) = p$ implique $p^u = 1$. Un raisonnement analogue à celui de la Proposition 6.5 donne le système de racines.

6.3. *Exemples numériques*

Les réseaux pairs unimodulaires de rang inférieur ou égal à 24 sont tous connus par un travail de Niemeier [**5**, Chapter 16]; ils ont tous pour rang un multiple de 8. En dimension 8 le seul est $\mathbb{E}_8$. Donc avec les notations de la Proposition 6.6: $B_2(3) = \mathbb{E}_8$. En dimension 24 il y a 24 réseaux qui sont caractérisés par leur système de racines:

$B_2(5)$ a un système de racines de type $(6)\mathbb{A}_4$,

$B_3(3)$ a un système de racines de type $(4)\mathbb{E}_6$.

Il se peut, qu'en général (pour tout p) B_2 puisse être caractérisé comme le seul réseau 'invariant' de l'algèbre de Lie $\mathrm{sl}(2, \mathbb{C})$ qui soit unimodulaire indécomposable et qui a un système de racines non-vide (voir [**2**]).

Bibliographie

1. E. BAYER-FLUCKIGER, 'Definite unimodular lattices having an automorphism of given characteristic polynomial', *Comment. Math. Helv.* 59 (1984) 509–538.
2. A. I. BONDAL *et al.*, 'Invariant lattices, the Leech lattice and its even unimodular analogues in the Lie algebras A_{p-1}', *Math. USSR Sbornik* 58 (1987) no. 2, 435–465.
3. N. BOURBAKI, *Groupes et algèbres de Lie* (Hermann, Paris, 1968), chapitres 4–6.
4. P. E. CONNER and R. PERLIS, *A survey of trace forms in algebraic number fields* (World Scientific, Singapore, 1984).
5. J. H. CONWAY and N. J. A. SLOANE, *Sphere packings, lattices and groups* (Springer, New York, 1988).
6. B. EREZ, 'Structure galoisienne et forme trace dans les corps de nombres', Thèse, Université de Genève, 1987.
7. B. EREZ, 'The Galois structure of the trace form in extensions of odd prime degree', *J. Algebra* 118 (1988) 438–446.
8. B. EREZ, 'The Galois structure of the square root of the inverse different', en préparation.
9. W. FEIT, 'On integral representations of finite groups', *Proc. London Math. Soc.* (3) 29 (1974) 633–683.
10. A. FRÖHLICH, *Galois module structure of algebraic integers*, Ergebnisse der Mathematik (3)1 (Springer, Heidelberg, 1983).

11. A. FRÖHLICH, *Classgroups and Hermitian modules,* Progress in Mathematics 48 (Birkhäuser, Boston, 1984).
12. J. MILNOR and D. HUSEMOLLER, *Symmetric bilinear forms,* Ergebnisse der Mathematik 73 (Springer, Heidelberg, 1973).
13. H.-G. QUEBBEMANN, 'Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung', *J. reine angew. Math.* 326 (1981) 158–170.
14. J.-P. SERRE, *Corps locaux,* 3ème édition (Hermann, Paris, 1968).
15. N. STOLZFUS, 'Unraveling the integral knot concordance group', *Mem. Amer. Math. Soc.* 12, 192 (1977) 1–91.
16. S. ULLOM, 'Normal bases in Galois extensions of number fields', *Nagoya Math. J.* 34 (1969) 153–167.
17. L. C. WASHINGTON, *Introduction to cyclotomic fields,* Graduate Texts in Mathematics 83 (Springer, New York, 1982).

Université de Bordeaux I
Laboratoire de Mathématiques
351, *Cours de la Libération*
F-33405 *Talence cedex*
France

Section de Mathématiques
Université de Genève
C.P. 240
Rue du Lièvre 2-4
CH-1211 *Genève* 24
Switzerland